REMARKS/ARGUMENTS

This amendment is submitted in response to the Final Office Action dated February 10, 2005. Claims 1-19 and 28-45 are pending in the present application. A telephone interview was conducted on February 4, 2005, between Examiner Thomas Ho and Applicant's Attorney, Stephen Sullivan. In response, claims 1-19 have been canceled to clarify issues for Appeal, and claim 28 has been amended to provide correct antecedent basis. Claims 28-45 remain pending.

Claim Rejections

The Examiner continues to reject claims 1-19, 28-29, 31-33, 35-44 under 35 U.S.C. §102 as being anticipated by U.S. Patent No. 5,778,071 issued to Caputo et al. The Examiner also continues to reject claims 30 and 34 under 35 U.S.C. §103 as being obvious. Applicant respectfully disagrees.

With the cancellation of claims 1 and 19, the focus of examination is on independent claims 28, 32, and 36. Independent claims 28 and 32, recite an authorization system in which a portable security device is removably coupled to a computer system to selectively authorize the use of computer programs on the host computer. The portable security device stores multiple items of authorization information that are used by the computer system to use the protected software programs and/or data. The portable security device includes a communication interface for communicating with multiple information authorities, such as software vendors, for downloading the authorization information to the portable security device for subsequent authorization of the vendor's software or data. The authorization information is then stored within a memory in the portable security device. When a user

wishes to authorize use of a protected program or data on the computer, the portable security device authorizes the computer system these the protected program or data only if the corresponding item of authorization is stored in the device.

Independent claim 36 recites an embodiment where the type of authorization information stored in the portable security device includes secret keys and key selectors for generating secret keys. Each item of authorization information stored in the device corresponds to a particular protected software program. When a user wishes to authorize use of a protected program or data on the computer, the computer transfers the key selector corresponding to the protected program or data to the portable security device. The portable security device then uses the key selector to generate the corresponding secret key, and then transfers the secret key to the computer for validation and release of the program or data.

Independent Claims 28 and 32 are not anticipated by Caputo

In order to sustain a rejection under §102, Caputo must disclose each and every element of rejected claims 23 and 32. Independent claims 28 and 32, which are similar in scope, are directed to a portable security device removably coupled to a computer system that has the following limitations:

1) stores multiple items of authorization information in memory,

2) each of the multiple items of authorization information must be associated with a respective item of protected information that is used by a computer system,

3) the portable security device must be capable of receiving multiple items of information while being coupled to the computer system (e.g., receiving updates or new authorization information), and

4) the portable security device must be capable of selectively authorizing the computer system to use one of the items of protected information based upon the corresponding item of authorization information being stored in the memory.

It is respectfully submitted that Caputo fails to teach or suggest each of the limitations of independent claims 28 and 32, and therefore fails to anticipate the present invention or render the present invention obvious.

First, Caputo fails to teach or suggest a device "for selectively authorizing the computer system to use multiple items of protected information," as recited in the preamble of claims 28 and 32. Instead, Caputo's device authorizes a user, not a computer system, to access a remote computer on a network. If servers on a network can verify the single identity of the device and/or the user, then access is granted. Caputo's device does not have the intelligence to determine what multiple pieces of information on the computer the user is allowed to access or not. Access is ultimately controlled by the servers on the computer network, which verify the user's PIN.

Caputo further fails to teach or suggest that the "multiple items of authorization information" "are associated with respective ones of the multiple items of protected information" on the computer to which the device is connected. The Examiner considers challenges and user PINs disclosed by Caputo to be analogous to the multiple items of protect information. Challenges are sent from a computer on a network to Caputo's device, and in response, the device prompts a user for a PIN or a smart card insertion. Challenges have nothing whatsoever to do with items of information that are associated with respective items of protected information, such as programs and data, on the computer to which computer's device is connected. Likewise, a PIN entered by the user or read from a smart card is associated with a user,

not to items of protected information on the computer.

Caputo also fails a teach or suggest that the "multiple items of authorization information" are "stored in the least one storage medium" of the portable device, as recited in claims 28 and 32. Instead, as described above, Caputo's challenges are sent from a computer over a network, and are not stored in the device, even once they are received. And Caputo's PINs are either entered by the user or read from a smartcard. User-entered PINs are not stored in Caputo's device, and although the PINs read from the smartcard are stored in the smartcard, the PINs are not stored in Caputo's device. In addition, because Caputo's challenges and PINs do not meet the limitation of "multiple items of authorization information" that are "associated with items of protected information", Caputo's challenges and PINs cannot be used to teach or suggest that the "multiple items of authorization information" are "receiv[ed]" after the device is "removably coupled to the computer," as recited in claims 28 and 32.

Caputo also fails to teach or suggest a portable security device for "selectively authorizing the computer system to use multiple items of protected information based upon the corresponding item of authorization information being stored in the storage medium," as recited in claims 28 and 32. As described above, Caputo's challenges and PINs are not stored within Caputo's device and Caputo's challenges and PINs are for allowing a user to access the network, rather than for allowing the computer to which it is connected to use items of protected information.

Because Caputo fails to teach or suggest each and every element of Claims 28 and 32, claims 28 and 32 are allowable over Caputo.

Independent Claim 36 is not anticipated by Caputo

Claim 36 recites a portable security device that stores multiple key selectors, one for each item of protected information on the computer to which it is connected. When the portable security device receives an authorization request from the computer system to authorize use of a particular one of the items of protected information, the stored key selector corresponding to the particular one of the items and a shared secret are used to generate authorizing information. Once the computer system validates the authorizing information, the particular one of the items of protect information is released for use by the computer system.

It is respectfully submitted that none of these recitations are taught or suggested by Caputo because Caputo fails to provide his device with "multiple" PINs, "one for each item of protected information" on the computer. In addition, neither Caputo's challenges or PINs are used to *generate* authorization information within the device, which is then validated by the computer to release the item of protected information.

Caputo also teaches cryptographic keys for encryption, where the encryption key can be calculated from the decryption key and vice versa to keep the key secret (col. 11, lines 17-38). However, these are standard encryption keys used for encrypting and decrypting data transmitted over the network. Any key used to generate another encryption/decryption key would be used only for that purpose, not for being validated by the computer system to release the item of protected information that key selector is associated with.

Accordingly, the reasons set forth above, it is respectfully summit that Caputo fails teach or suggest independent claim 36.

Examiner concerns

During the February 4, 2005 interview, the Examiner expressed two primary concerns with the claims: 1) that the claims may be met by multiple dongles daisy chained together and coupled to a computer system, where each dongle has a single authorization, and 2) that the claims may be met by a smartcard having multiple authorizations.

Although Applicants thank the Examiner for clarifying his position, it is respectfully submitted that the Examiner has cited no prior art reference disclosing such teachings. In addition, it seems that the expression of these concerns may be interpreted as an admission that Caputo is an insufficient reference to maintain a rejection of the claims. Nevertheless, the Examiner's concerns are addressed below along with a continued explanation of why Caputo fails teach or suggest each every element of the claims.

Independent Claims 28 and 32 are not met by multiple dongles daisy chained together

First, it should be pointed out that both of the Examiner's concerns with respect to potential prior art are distinguished in the Background of the invention of the present application, which describes the disadvantages of both dongles and smart cards.

With respect to dongles, the Background states:

> However, a disadvantage presented by dongles is that they typically store authorization information for only one software program or perhaps for a group of software programs from a single vendor. Consequently, because an end-user typically might use several software programs from multiple vendors at any given time, he or she might have to carry around multiple dongles, which could be cumbersome and inconvenient.
>
> Another disadvantage is that the authorization information stored in the dongle is typically set by the software vendor during manufacture and generally cannot be subsequently updated. As a result, when a software vendor provides an end-user with a software upgrade, add-on or plug-in,

> etc. for a protected software program, the vendor often also delivers a new dongle to authorize the associated software. This is not very cost-effective for software vendors because the cost of the dongle itself can be significant in relation to the value of the associated software. (Page 2, lines 16-29)

With respect to the Examiner's concern that the claims may be met by multiple daisy chained dongles, it is respectfully submitted that claims 28 and 32 recite "a portable secure device," rather than multiple portable security devices, and that interpreting the claim to be anticipated by multiple devices that are daisy-chained together is improper.

The Examiner admits that he could find no reference that teaches a single dongle having multiple authorizations. As described in the Background, a single dongle can only authorize the use of one program, and to authorize multiple programs by daisy chaining single dongles together would require a user to carry around multiple dongles, which would be cumbersome and inconvenient.

The present invention overcomes this problem by providing a portable security device that holds and formalizes access to multiple authorizations. The innovation here is that where it used to take many devices to authorize the same number of protected software products, it now only takes one security device of the present invention.

It is respectfully submitted that multiple single-authorization devices daisy-chained together fails to teach or suggest the device of the present invention for the following reasons:

First, unlike single-authorization devices, a multi-authorization device has to include a mechanism for selecting the proper authorization that corresponds to the correct item of protected information. This is analogous to a jukebox which has a

mechanism to select a record chosen by a user. With multiple daisy-chained single-authorization devices, a mechanism must exist for selecting the proper authorization, and the Examiner has not explained nor pointed to any reference describing how this would be done. Most likely, this would be done using an application running on the host computer. Since the authorization would take place on the host computer, rather than in the devices, the system would fail to teach or suggest a portable security device that "selectively authorize[es] the computer system to use one of the items of protected information based upon the corresponding item of authorization information being stored in the memory," as claimed.

Second, the system proposed by the Examiner is not enabled and would fail to disclose inherent properties of the claimed portable security device. For example, one inherent property of the portable security device is that it allows different "information authorities" (e.g., vendors) to store authorizations in the device without conflicts. In contrast, multiple single-authorization devices connected to the computer may interfere with each other because there is no mechanism to coordinate the different devices. The Examiner has also failed to explain or cite a reference describing how the authorizations would be handled in the daisy-chained single-authorization device system such that there are no conflicts between the devices.

The daisy-chained single-authorization device system suggested by the Examiner also fails to teach or suggest "an interface capable of receiving multiple items of authorization information," as recited in claim 28, which also requires that the device be coupled to the computer system is to use the multiple items of protected information. This implies that authorizations can be added to the portable security device *after* the device has been sent to the end-user and coupled to the user's computer. The daisy-

chained single-authorization device system lacks this property.

Another inherent property of the portable security device is that the size of its memory is the only limitation on the number of authorizations it can hold. In contrast, the daisy-chained single-authorization device system is limited because the computer system to which the devices are connected is limited in the number of devices that it can handle simultaneously. Using devices that hold one authorization limits the computer to only simultaneously accessing the same number of authorized programs as devices connected to the computer. With the parallel port devices, only a few devices could be used. Even with a USB port, 127 is the maximum number of connected devices possible. In industries where software plug-ins for a software application are protected with separate authorizations, it is not uncommon to exceed 127 authorizations. The claimed portable secure device of the present invention does not face this restriction.

Accordingly, it is respectfully submitted that the daisy-chained single-authorization device system would fail teach or suggest the claims of the present invention.

Independent Claims 28 and 32 are not met by smartcards

Smartcards are distinguished from the present invention in the Background of the Invention, which states.

> A third technique described in U.S. Patent No. 5,854,891, issued to Postlewaite ("the '891 patent") describes a security device for enabling selected functions to be performed by or within a computer connected to the security device. The security device includes a smart card reader for reading data from smart cards, which may be considered to be a type of information authority...
>
> However, the security device of the '891 patent suffers from several

> disadvantages. First, the security device requires a "segmented" memory to prevent the smart cards stored in the memory from interfering with each other and possibly corrupting one another's data. This increases the complexity and cost of the security device because it necessitates that the device implement memory management or protection mechanisms in hardware and/or software. Second, the security device apparently is not capable of receiving authorization information from multiple types of information authorities. The '891 patent mentions that the security device can receive enabling data or authorization information from smart cards. However, the patent does not disclose or suggest that the device can receive authorization information from other types of information authorities, such as floppy disks or computer servers. Consequently, it appears that the use of the security device as an authorization device is limited to those software vendors that support smart cards as a data delivery mechanism. (Page 4, line 1 through page 5, line2).

A smartcard having multiple authorizations fails to teach or suggest the claimed portable security device of the present invention for several additional reasons. First, a smartcard loaded with multiple authorizations cannot be used by itself to authorize items of protected information on a computer. Instead, a smartcard reader must be connected to the computer that reads the smartcard and passes the authorization information to the computer. Therefore, any smartcard system requires two components rather than one, the smartcard and the smartcard reader, and therefore fails to meet the "a portable security device" limitation of claims 28 and 32. If anything, it is the smartcard reader that is more analogous to the claimed portable security device since it is connected to the host computer. However, the smartcard reader does not “store” the "multiple items of authorization information," rather the smartcard does.

Also, as with the daisy-chained single-authorization device system, the Examiner has not described or pointed to a reference that describes a mechanism for selecting the proper authorization from among all the authorizations on the smartcard when

authorizing one of the items of protected information on the computer. As described above, the most likely mechanism would be an application running on the host computer. Since the authorization would take place on the host computer, rather than in the devices, the system would fail to teach or suggest a portable security device that "selectively authorize[es] the computer system to use one of the items of protected information based upon the corresponding item of authorization information being stored in the memory," as recited in claims 28 and 32. The Arguments above apply with full force and effect to independent claim 36.

Accordingly, it is respectfully submitted that a Smartcard having multiple authorizations fail to teach or suggest the claims of the present invention.

In view of the foregoing, it is submitted that claims independent claims 28, 32 and 36 are allowable over the cited reference. Because the dependent claims are based on allowable independent claims, the dependent claims are allowable as well. Accordingly, Applicant respectfully requests reconsideration and passage to issue of claims 28-45 as now presented.

Applicants' attorney believes that this Application is in condition for allowance. Should any unresolved issues remain, the Examiner is invited to call Applicants' attorney at the telephone number indicated below.

Respectfully submitted,

SAWYER LAW GROUP LLP

April 11, 2005
Date

Stephen G. Sullivan.
Attorney for Applicant(s)
Reg. No. 38,329
(650) 493-4540